(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 747 208**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 04404**

(51) Int Cl[6] : **G 06 F 1/00**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 09.04.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 10.10.97 Bulletin 97/41.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *CLEMOT OLIVIER* — FR, *CAMPANA MIREILLE* — FR et *ARDITTI DAVID* — FR.

(72) **Inventeur(s) :**

(73) **Titulaire(s) :** .

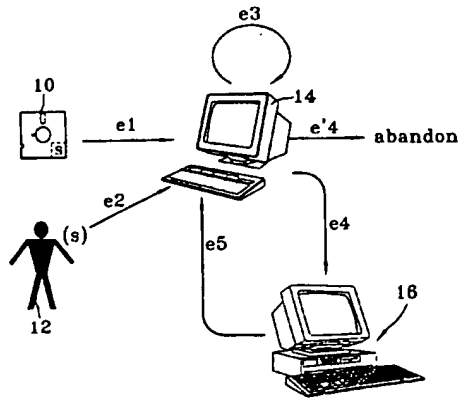
(74) **Mandataire :** SOCIETE DE PROTECTION DES INVENTIONS.

(54) PROCEDE DE DISSIMULATION D'UN CODE SECRET DANS UN DISPOSITIF D'AUTHENTIFICATION INFORMATIQUE.

(57) L'invention concerne un procédé de dissimulation d'un code secret dans un dispositif d'authentification informatique (10) consistant à crypter le code secret (s) par une fonction de cryptage (g) pour former une image de code secret (s) et à mémoriser cette image de code secret dans le dispositif d'authentification. Il consiste, au préalable, à choisir une fonction de cryptage (g) qui est telle que, à chaque image de code secret mémorisée, il correspond une pluralité de codes antécédents (s1, ..., sn) tous différents du code secret, mais qui, une fois cryptés par la fonction de cryptage (g), ont une image (s) identique à celle du code secret.

Elle concerne aussi un procédé de vérification du code secret d'un utilisateur muni d'un dispositif d'authentification dans lequel est mémorisée l'image du code secret.

Application au domaine de l'authentification informatique.



FR 2 747 208 - A1

PROCEDE DE DISSIMULATION D'UN CODE SECRET DANS UN DISPOSITIF D'AUTHENTIFICATION INFORMATIQUE

DESCRIPTION

Domaine technique

L'invention concerne un procédé pour dissimuler un code secret dans un dispositif d'authentification tel qu'une disquette informatique, une carte à mémoire,..., pouvant être lu à partir d'un lecteur adéquat.

Elle trouve des applications dans tous les systèmes informatiques mettant en oeuvre une procédure d'authentification des utilisateurs voulant se connecter, depuis un terminal, sur le système central.

Etat de la technique

Dans les systèmes informatiques actuels, la protection des données joue un rôle de plus en plus important. En effet, la qualité du système informatique dépend de manière décisive de la sécurité de l'échange de données à l'intérieur du système. On cherche donc de plus en plus à sécuriser l'accès au système, c'est-à-dire que l'on cherche à contrôler si les personnes utilisant le système sont autorisées à l'utiliser, les personnes non autorisées devant alors être refusées par le système.

Un mode de réalisation simple, mais n'offrant pas une sécurité absolue, consiste à contrôler l'accès au système informatique par la vérification du mot de passe connu uniquement de l'utilisateur autorisé et souvent changé afin de limiter la possibilité que des utilisateurs non autorisés découvrent ce mot de passe. Cependant, il y a de forts risques pour que les mots de passe soient

interceptés par des personnes non autorisées désireuses d'utiliser le système informatique.

De plus, ce mot de passe est stocké dans la zone mémoire du système informatique (zone protégée ou non) afin d'être comparé au mot de passe entré par l'utilisateur. Il peut donc être facilement retrouvé en mémoire par un utilisateur frauduleux.

Pour éviter cette fraude, une technique consiste à crypter le mot de passe avant de le stocker en mémoire. Ce cryptage se fait au moyen d'une fonction de cryptage qui est choisie, en général, de façon à ce qu'il soit impossible de retrouver le mot de passe à partir de l'image du mot de passe obtenue après cryptage de ce mot de passe. Cette technique est utilisée, par exemple, dans les systèmes UNIX®.

Dans ce cas, l'image du mot de passe est stockée en clair dans la mémoire de sorte qu'il est possible à un utilisateur frauduleux de récupérer le fichier de toutes les images de mots de passe mémorisées et ensuite d'implémenter la fonction de cryptage sur un autre système informatique et d'essayer des listes de mots de passe jusqu'à retrouver ceux qui correspondent aux images du fichier. Une telle analyse du code du système (fonction, fichier des images de mot de passe...) est appelée "attaque par dictionnaire".

Par ailleurs, il existe un procédé permettant de dissimuler un code secret en stockant, sur des moyens de stockage tels qu'une disquette, une carte à mémoire, etc., l'image du code secret par une fonction de cryptage réversible, paramétrée par le mot de passe de l'utilisateur. Ce procédé est mis en oeuvre "localement", c'est-à-dire qu'il est exécuté par le terminal, en liaison avec les moyens de stockage et qu'il ne nécessite aucune connexion vers le système central.

Ce procédé est décrit en détail dans la demande de brevet FR-A-2 690 257.

Comme expliqué dans cette demande de brevet, ce procédé permet aussi de changer le mot de passe de l'utilisateur localement, c'est-à-dire sans qu'aucune connexion au système central ne soit nécessaire. Par contre, une connexion au système est obligatoire pour vérifier la validité de ce changement de mot de passe.

L'authentification de l'utilisateur se fait donc localement : le code secret n'est jamais transmis, sur une ligne de transmission, vers le système central. L'unique transmission du code secret au cours du procédé, se fait entre le lecteur des moyens de stockage et le terminal, ce qui limite les risques d'interception par un fraudeur. La connexion sur le système central se fait ensuite, c'est-à-dire après vérification locale du code secret.

Cependant, un tel procédé nécessite une protection physique des moyens de stockage (disquette) pour éviter la fraude directement sur ces moyens de stockage. Ceci implique donc l'utilisation de matériels et de technologies spécifiques, entraînant un coût relativement important.

Exposé de l'invention

L'invention a pour but de remédier aux inconvénients des procédés décrits précédemment. A cette fin, elle propose un procédé pour dissimuler un code secret dans un dispositif d'authentification tel qu'une disquette ou une carte à mémoire. Ce procédé permet de vérifier localement le code secret entré par l'utilisateur, tout en limitant les risques d'attaques par dictionnaire.

De façon plus précise, l'invention concerne un procédé de dissimulation d'un code secret dans un dispositif d'authentification informatique consistant à

crypter le code secret par une fonction de cryptage pour former une image de code secret et à mémoriser cette image de code secret dans le dispositif d'authentification. Ce procédé se caractérise par le fait qu'il consiste, au préalable, à choisir une fonction de cryptage qui est telle que, à chaque image de code secret, il correspond une pluralité de codes antécédents tous différents du code secret, mais qui, une fois cryptés par la fonction de cryptage, ont une image identique à celle du code secret.

Avantageusement, le code secret ayant n caractères, la fonction de cryptage consiste à associer à ces n caractères une image de code secret de k caractères, avec $k < n$.

Selon un mode de réalisation préféré de l'invention, le nombre k des caractères de l'image du code secret est égal à $\frac{n}{2}$.

L'invention concerne aussi un procédé de vérification du code secret d'un utilisateur voulant accéder à un système central à partir d'un terminal. Cet utilisateur étant muni d'un dispositif d'authentification dans lequel est dissimulée l'image du code secret par la fonction de cryptage, ce procédé se caractérise par le fait qu'il comprend une étape de vérification locale du code secret entré par l'utilisateur et crypté par la fonction de cryptage, par comparaison avec l'image du code secret mémorisée dans le dispositif d'authentification ; puis, si cela est vérifié, il comporte une étape d'authentification par le système central.

Brève description des figures

- La figure 1 représente schématiquement la répartition des images du code secret dans la mémoire ainsi que des antécédents possibles de cette image ;

- les figures 2A, 2B, 3A et 3B représentent des exemples de fonctions de cryptage appliquées à un certain nombre de caractères numériques ; et

- la figure 4 représente le schéma fonctionnel du procédé de vérification du code secret.

Description détaillée de modes de réalisation de l'invention

L'invention concerne un procédé pour dissimuler un code secret dans un dispositif d'authentification tel qu'une disquette informatique ou une carte mémoire ou encore une calculette.

Ce procédé consiste à crypter le code secret par une fonction de cryptage g, de façon à former une image du code secret qui est ensuite mémorisée dans le dispositif d'authentification.

La fonction de cryptage g est choisie de façon à ce que l'image du code secret soit suffisamment précise pour qu'une faute de frappe, tapée par l'utilisateur lorsque celui-ci entre son code secret, puisse être détectée avec une probabilité tout à fait satisfaisante mais que, pourtant, chaque image du code secret possède de nombreux antécédents par la fonction de cryptage, de façon à ce qu'une attaque par dictionnaire fournisse de nombreuses fausses solutions à la vérification locale, mais pas à l'authentification distante.

En d'autres termes, la fonction de cryptage g est choisie de façon à ce que le code secret ait une image de code secret qui corresponde à une multitude de codes antécédents (appelés simplement "antécédents", dans la suite du texte). Ces codes antécédents sont une sorte de faux codes secrets, qui, codés par la fonction de cryptage g, donnent tous la même image de code secret que le

véritable code secret de l'utilisateur, mais qui seront refusés lors de la procédure d'authentification.

Ainsi, un utilisateur frauduleux qui serait en possession du dispositif d'authentification, par exemple de la disquette, et qui aurait ainsi découvert le fichier des images de codes secrets et qui, par ailleurs, serait en possession de la fonction de cryptage g, ne pourrait pas déterminer précisément quel est le code secret de l'utilisateur. En effet, une attaque par dictionnaire lui fournirait de nombreuses solutions à la vérification locale, mais une très faible chance de trouver la véritable solution, c'est-à-dire le véritable code secret. Effectivement, si l'utilisateur frauduleux essaie l'un des codes antécédents fourni par l'attaque par dictionnaire, celui-ci est vérifié localement ; par contre, il sera refusé lors de l'authentification à distance, c'est-à-dire de l'authentification par le système central.

On a représenté sur la figure 1, de façon très schématique, la répartition des images de codes secrets dans la mémoire, ainsi que la répartition des codes antécédents de ces images de codes secrets.

De façon plus précise, on a appelé "E1" l'ensemble de tous les codes qui pourraient être un code secret choisi par l'utilisateur et "E2" l'ensemble de toutes les images de ces codes secrets qui pourraient être choisis par l'utilisateur. L'ensemble E1 comporte donc tous les éventuels codes secrets, dont, en particulier, un code x et une multitude de codes s1 à sn.

Si "g" est la fonction de cryptage choisie, alors l'image du code x par la fonction de cryptage g donne l'image X qui se situe dans l'ensemble E2 des images de codes secrets possibles. D'autre part, l'image par la fonction de cryptage g de chacun des codes s1 à sn donne l'image de code secret S contenue dans l'ensemble E2.

Ce sont donc tous ces codes antécédents s1, s2, s3,..., sn qui, codés par la fonction de cryptage g, donnent une image S qui correspond aussi à l'image du véritable code secret. On comprend donc que l'un de ces codes s1 à sn est le véritable code secret choisi par l'utilisateur. Ainsi, bien que tous ces codes antécédents s1 à sn aient pour image S, l'un seulement de ces codes antécédents est le véritable code secret qui vérifiera l'authentification par le système central.

Ainsi, un utilisateur frauduleux qui serait en possession à la fois de la fonction de cryptage g et de l'image de code secret S, ne saura lequel des codes antécédents s1 à sn choisir. Aussi, s'il essaie localement, c'est-à-dire au niveau du terminal informatique, l'un de ces codes antécédents s1 à sn, la vérification par le terminal lui donnera une réponse positive, c'est-à-dire qu'une procédure d'authentification peut être mise en oeuvre. Cependant, cette procédure d'authentification n'aboutira pas et la connexion au système central sera refusée.

Par contre, la fonction de cryptage est choisie de façon à ce qu'elle fournisse des images de codes secrets suffisamment précises pour qu'une faute de frappe de la part de l'utilisateur puisse être détectée localement, c'est-à-dire sans nécessiter de connexion avec le système central.

Selon un mode de réalisation de l'invention, la fonction de cryptage g est une fonction qui associe à n caractères constituant le code secret, une image de code secret de taille réduite, c'est-à-dire de k caractères, avec $k < n$. Par exemple, pour un code secret ayant n caractères, la fonction de cryptage g associe une image de $k = n/2$ caractères. Dans le mode de réalisation préféré de l'invention, la fonction g associe à un code secret de huit

caractères (ce qui correspond à une taille d'environ 2^{40} bits), une image de code secret de quatre caractères (taille d'environ 2^{20} bits).

Pour une fonction de cryptage g de ce type, l'utilisateur qui tape le véritable code secret avec une faute de frappe aura un risque sur environ un million de cas (1 sur 2^{20}) que sa faute de frappe ne soit pas détectée lors de l'opération de vérification locale ; par contre, un utilisateur frauduleux qui tente une attaque par dictionnaire se verra confronté à environ un million de solutions (2^{20}), parmi lesquelles une seule est la bonne, c'est-à-dire qu'une seule correspond au véritable code secret.

On comprendra, bien sûr, que plusieurs fonctions peuvent être utilisées, pour vérifier les conditions énoncées précédemment. Même des fonctions très simples peuvent être utilisées. Par exemple, si l'on prend en compte les chiffres entre 0 et 9 et les lettres de l'alphabet que l'on représente par des valeurs comprises entre 10 et 35, on peut choisir une fonction g1 qui associe, à chaque couple de caractères (lettres ou chiffres) du code secret de l'utilisateur, une valeur déterminée entre 0 et 35, de telle sorte que pour un caractère donné du bigramme (c'est-à-dire du couple de caractères), l'image soit différente lorsque le deuxième caractère varie. On peut, par exemple, choisir la somme des deux valeurs du bigramme.

La figure 2A représente schématiquement le traitement effectué par la fonction g1 sur un code secret comprenant n caractères.

On a donc représenté sur cette figure 2A, les n/2 couples de caractères (c1, c2) (c3, c4)... (c1, cn) et chacune des images $Ic_1, \ldots, Ic_{n/2}$ de ces bigrammes. D'après la définition de la fonction g1, décrite précédemment,

chaque image $Ic_{n/2}$ correspond à la somme des caractères C_1 et C_n du bigramme correspondant, sachant que si la somme de ces caractères donne une valeur supérieure ou égale à 10, on choisit pour $Ic_{n/2}$ la valeur de plus faible poids, à savoir le chiffre de l'unité.

La figure 2B représente un exemple numérique du cryptage réalisé au moyen de la fonction g1. Dans cet exemple, on considère un code secret de huit caractères numériques notés c1, c2,..., c8 regroupés en quatre bigrammes dont les valeurs sont comprises entre 0 et 9 sont :

(c1, c2) = (6,1)
(c3, c4) = (5,7)
(c5, c6) = (4,3)
(c7, c8) = (9,2)

La fonction g1 associe donc à chaque bigramme, la somme des deux caractères le constituant. Ainsi :

Σ(c1, c2) = 7
Σ(c3, c4) = 2
Σ(c5, c6) = 7
Σ(c7, c8) = 1

On comprend donc, à partir de cet exemple, que l'image du code secret "61574392" est "7271". Une telle image 7271 peut avoir une multitude d'antécédents, puisque chaque caractère de cette image du code secret peut être le résultat de la somme (ou bien l'unité d'un chiffre correspondant à la somme) d'une multitude de nombres compris entre 0 et 35.

On comprend bien, de plus, que si l'utilisateur tapait le véritable code secret avec une erreur de frappe, par exemple 7 à la place de 6 pour le caractère c1, cette erreur serait tout de suite détectée localement puisque la somme de 7 et de 1 ne peut, bien évidemment, donner le

chiffre 7 qui correspond à l'image Ic1 du premier couple de caractères (c1, c2).

Sur la figure 3A, on a représenté un exemple d'une autre fonction de cryptage : la fonction g_2 qui consiste à associer à l'ensemble des huit caractères c1 à C8 composant le code secret, quatre combinaisons linéaires indépendantes, modulo 36, de ces huit caractères, chaque combinaison linéaire pouvant être différente.

Par exemple, le premier caractère Ic1 de l'image du code secret associe les caractères c1, c3, c4 et c7 du code secret ; le second caractère Ic2 de cette image du code secret associe les caractères c2, c5, c6 et c8 ; le troisième caractère de l'image du code secret Ic3 associe les caractères c1, c2, c5 et c7, et le quatrième caractère Ic4 de l'image du code secret associe les caractères c3, c4, c5 et c7 du code secret initial.

Sur la figure 3B, on a représenté le même exemple que celui de la figure 3A, mais dans lequel on a attribué à chaque caractère une valeur numérique qui est la même que celle donnée dans l'exemple de la figure 2B. Ainsi :

c1 = 6
c2 = 1
c3 = 5
c4 = 7
c5 = 4
c6 = 3
c7 = 9
c8 = 2

Après cryptage, par la fonction g2, d'un code secret de huit caractères c1 à c8, où c1,..., c8 ont les valeurs ci-dessus, on obtiendra une image de code secret 7007, avec Ic1 = 7, Ic2 = 0, Ic3 = 0, Ic4 = 7.

Ainsi, le procédé de dissimulation du code secret sur le dispositif d'authentification présente donc l'avantage, non seulement de détecter une éventuelle faute de frappe de la part de l'utilisateur lorsque celui-ci entre son code secret sur le terminal, mais surtout d'éviter une attaque par dictionnaire de la part d'un utilisateur frauduleux, puisque l'image du code secret mémorisée sur la disquette à un tel nombre de codes antécédents possibles qu'un utilisateur frauduleux a très peu de chance de trouver le véritable code secret.

Le procédé décrit ci-dessus pour dissimuler un code secret dans une disquette informatique, une carte à mémoire, ou tout autre dispositif d'authentification, peut être utilisé dans un procédé de vérification du code secret entré par un utilisateur désirant accéder à un système central, à partir d'un terminal connecté à un lecteur apte à lire son dispositif d'authentification.

Pour une meilleure compréhension de l'invention, le procédé de vérification du code secret va être décrit dans le cas où le dispositif d'authentification est une disquette informatique.

Ce procédé de vérification consiste, après que la disquette ait été introduite dans le lecteur de disquettes associé au terminal, à ce que l'utilisateur entre son code secret sur le terminal à partir duquel il désire se connecter au système central. Le terminal vérifie alors si l'image, par la fonction de cryptage g, du code secret s que vient de taper l'utilisateur correspond à l'image S mémorisée sur la disquette. Si cela n'est pas le cas, alors le terminal refuse toute connexion vers le système central. Au contraire, si cela est vérifié, alors une étape de détermination de la clé secrète non chiffrée K est commencée, au terme de laquelle le terminal se connectera au système central. Cette clé secrète non

chiffrée K est déterminée à partir de l'inverse f^{-1} de la fonction de chiffrage f de la clé par le mot de passe (f étant une fonction réversible), et à partir de la clé chiffrée stockée sur la disquette, tel que cela est expliqué dans la demande de brevet FR-A-2 690 257, déjà citée précédemment.

La procédure d'authentification qui est mise en oeuvre dès que le terminal informatique se connecte sur le système central, ne sera donc pas décrite ici puisqu'elle est identique à celle décrite dans le document FR-A-2 690 257.

Un diagramme fonctionnel de ce procédé de vérification du code secret est représenté sur la figure 4.

La disquette informatique, référencée 10, est introduite dans le terminal informatique 14 lors d'une étape e1. L'utilisateur, référencé 12, entre ensuite son code secret (s) sur le terminal 14 lors d'une étape e2. Une étape e3 est alors effectuée qui consiste à crypter par la fonction g, le code secret s que l'utilisateur vient d'entrer puis à vérifier si l'image du code secret par la fonction g correspond bien à l'image de code secret s mémorisée sur la disquette 10. Si ce n'est pas le cas, alors le procédé de vérification est abandonné (étape e'4) et donc aucune procédure d'authentification par le système central n'est envisagée. Au contraire, si cette vérification s'avère exacte, une étape e4 est effectuée. Cette étape e4 consiste à déterminer la clé secrète non chiffrée K et à l'envoyer au système central 16 qui commence alors la procédure d'authentification (étape e5), au moyen d'un échange d'informations avec le terminal 14.

Ainsi, le procédé de vérification du code secret assure une limitation du nombre de connexions au système central, puisque seuls les codes secrets acceptés lors de la vérification locale du code secret font l'objet d'une procédure d'authentification.

De plus, l'image du code secret étant mémorisée sur le dispositif d'authentification, et non dans une mémoire accessible à tous un utilisateur frauduleux désirant connaître cette image de code secret doit tout d'abord s'emparer de ce dispositif d'authentification, ce qui participe à la limitation des fraudes.

REVENDICATIONS

1. Procédé de dissimulation d'un code secret dans un dispositif d'authentification informatique (10) consistant à crypter le code secret (s) par une fonction de cryptage (g) pour former une image de code secret (s) et à mémoriser cette image de code secret dans le dispositif d'authentification, caractérisé en ce qu'il consiste, au préalable, à choisir une fonction de cryptage (g) qui est telle que, à chaque image de code secret mémorisée, il correspond une pluralité de codes antécédents (s1,..., sn) tous différents du code secret, mais qui, une fois cryptés par la fonction de cryptage (g), ont une image (s) identique à celle du code secret.

2. Procédé de dissimulation d'un code secret selon la revendication 1, caractérisé en ce que le code secret ayant n caractères (c1,..., cn), la fonction de cryptage (g) consiste à associer à ces n caractères (c1,..., cn) une image de code secret de k caractères, avec $k < n$.

3. Procédé de dissimulation d'un code secret selon la revendication 2, caractérisé en ce que le nombre k des caractères de l'image du code secret est égal à $\frac{n}{2}$.

4. Procédé de vérification du code secret d'un utilisateur voulant accéder à un système central à partir d'un terminal, caractérisé en ce que, cet utilisateur (12) étant muni d'un dispositif d'authentification (10) dans lequel est mémorisée l'image (s) du code secret par la fonction de cryptage (g) conformément à l'une quelconque des revendications 1 à 3, il comprend une étape (e3) de vérification locale du code secret entré par l'utilisateur et crypté par la fonction de cryptage, par comparaison avec l'image du code secret mémorisée dans le dispositif d'authentification, puis si cela est vérifié, une étape (e5) d'authentification par le système central (16).

FIG. 1

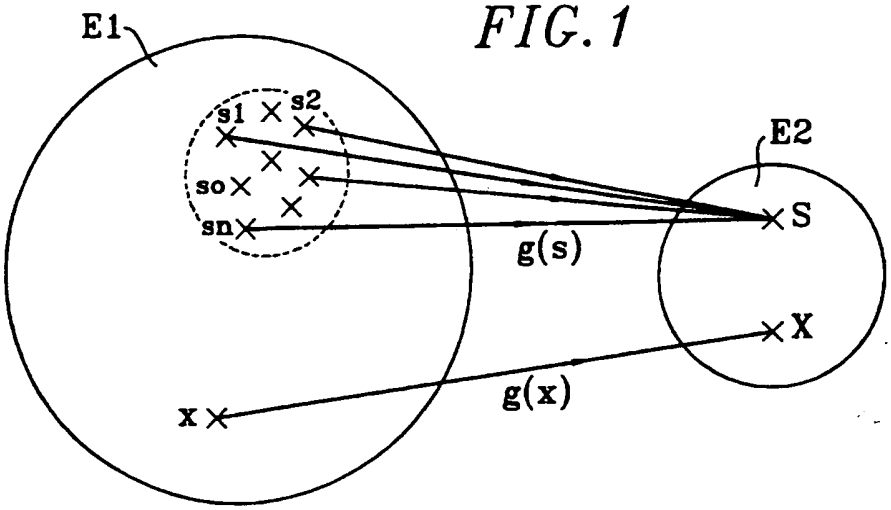
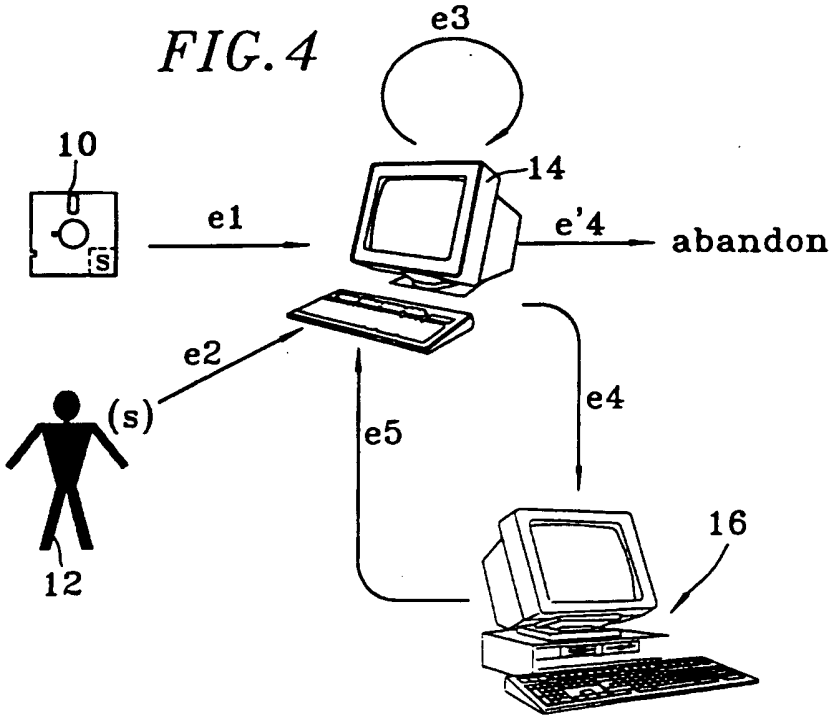


FIG. 4



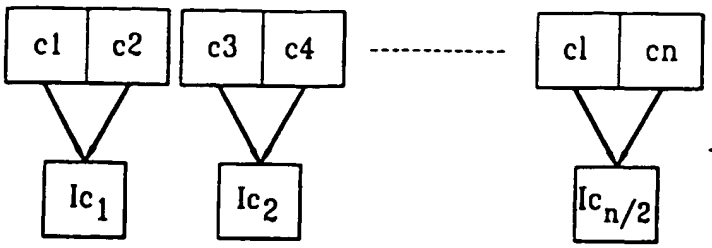


FIG.2A

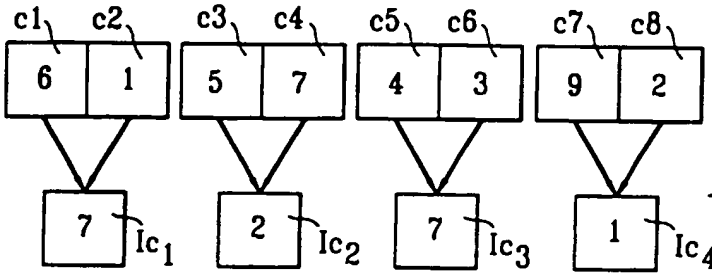


FIG.2B

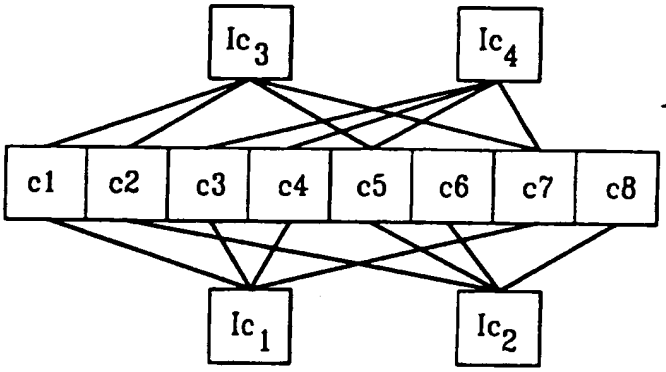


FIG.3A

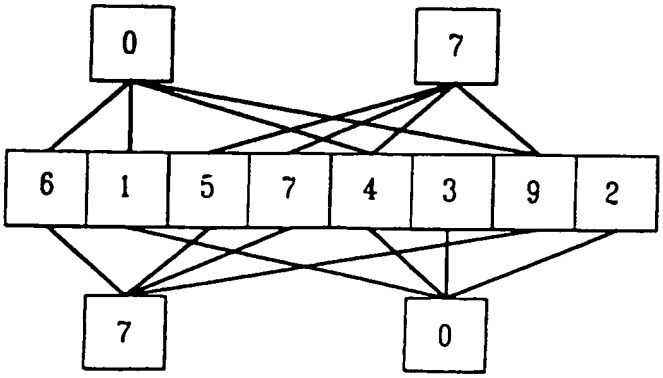


FIG.3B

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2747208
N° d'enregistrement national

FA 530538
FR 9604404

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	EP-A-0 191 324 (IBM) 20 Août 1986 * abrégé; figures 1,2 * * colonne 2, ligne 42 - colonne 3, ligne 7 * * revendication 1 *	1-3
A	---	4
Y	COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 11, no. 5, 1 Septembre 1992, pages 427-437, XP000296996 BAUSPIESS F ET AL: "REQUIREMENTS FOR CRYPTOGRAPHIC HASH FUNCTIONS" * le document en entier *	1-3
A	---	4
A	PHILIPS TELECOMMUNICATION REVIEW, vol. 47, no. 3, 1 Septembre 1989, pages 1-19, XP000072642 FERREIRA R C: "THE SMART CARD: A HIGH SECURITY TOOL IN EDP" * figures 4,6 * * page 5, ligne 6 - page 7, ligne 5 * * page 9, ligne 1 - page 11, ligne 4 *	1,4
A	---	2,3
A	US-A-5 233 655 (SHAPIRO SANFORD S) 3 Août 1993 * abrégé *	
D,A	---	1,4
	FR-A-2 690 257 (FRANCE TELECOM ;ALLEGRE FRANCOIS; ARDITTI DAVID; CAMPANA MIREILLE) 22 Octobre 1993 * le document en entier *	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G06F
H04L

Date d'achèvement de la recherche: 19 Décembre 1996

Examinateur: Powell, D

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

PTO 00-3045

CY=FR DATE=19971010 KIND=A1
PN=2,747,208

PROCESS FOR THE CONCEALMENT OF A SECRET CODE IN A COMPUTER AUTHENTICATION DEVICE
[Procédé de dissimulation d'un code secret dans un dispositif d'authentication informatique]

OLIVIER CLEMOT, et al.

UNITED STATES PATENT AND TRADEMARK OFFICE
Washington, D. C. June 2000

Translated by: FLS, Inc.

PUBLICATION COUNTRY	(10):	FRANCE
DOCUMENT NUMBER	(11):	2747208
DOCUMENT KIND	(12):	A1
PUBLICATION DATE	(43):	19971010
PUBLICATION DATE	(45):	
APPLICATION NUMBER	(21):	9604404
APPLICATION DATE	(22):	19960409
ADDITION TO	(61):	
INTERNATIONAL CLASSIFICATION	(51):	G06F 1/00
DOMESTIC CLASSIFICATION	(52):	
PRIORITY COUNTRY	(33):	
PRIORITY NUMBER	(31):	
PRIORITY DATE	(32):	
INVENTOR	(72):	NOT NAMED
APPLICANTS	(71):	CLEMOT, OLIVIER; CAMPANA, MIREILLE; ARDITTI, DAVID
TITLE	(54):	PROCESS FOR THE CONCEALMENT OF A SECRET CODE IN A COMPUTER AUTHENTICATION DEVICE
FOREIGN TITLE	(54A):	PROCÉDÉ DE DISSIMULATION D'UN CODE SECRET DANS UN DISPOSITIF D'AUTHENTICATION

PROCESS FOR THE CONCEALMENT OF A SECRET CODE IN A COMPUTER AUTHENTICATION DEVICE

/1*

SPECIFICATION

Technical field

The invention concerns a process for the concealment of a secret code in an authentication device, such as a computer diskette, a memory card, ... which can be read with an adequate reader.

It finds application in all computer systems implementing a procedure for the authentication of users desiring to be connected to the central system from a terminal.

State of the art

In current computer systems, the protection of data is playing an ever more important role. In fact, the quality of the computer system depends in a crucial way upon the security of data exchange within the system. An ever greater effort is thus being made to secure access to the system, that is to say, the effort is made to check whether those persons utilizing the system are authorized to use it, unauthorized persons then being rejected by the system.

One simple execution mode, which does not however offer absolute security, consists of controlling access to the computer system by the verification of the password, known only to the authorized user and frequently changed in order to reduce the

---

*Numbers in the margin indicate pagination in the foreign text.

possibility that unauthorized users will discover the password. Nevertheless, there is high risk that passwords will be /2 intercepted by unauthorized persons desiring to use the computer system.

Moreover, the password is stored in the memory zone of the computer system (protected or unprotected zone) in order to be compared with that password entered by the user. It can then be easily retrieved from memory by a fraudulent user.

To avoid this deception, one technique consists of encrypting the password before it is stored in memory. This encryption is accomplished by an encryption function which is selected, in general, in such a way that it will be impossible to retrieve the password from the password image obtained after encryption of that password. This technique is utilized, for example, in the UNIX® system.

In that case, the password is stored in memory in cleartext, so that it is possible for unauthorized users to retrieve the file containing all the password images in memory and then to implement the encryption function on a different computer system, testing the password lists until those corresponding to the images in the file are found. Such an analysis of the system code (function, password-image file...) is called an "attack by dictionary".

On the other hand, there does exist a procedure permitting the concealment of a secret code by storing the image of the secret code, on a storage means such as a diskette, a memory

card, etc., by means of a reversible encryption function parameterized by the user password. This procedure is implemented "locally", that is to say, it is executed by the terminal in conjunction with the storage means and requires no connection with the central system.

This procedure is described in detail in patent application FR-A 2,690,257. /3

As explained in that patent application, this procedure also permits changing the user password locally, that is to say, with no connection to the central system being necessary. However, a connection to the central system is required in order to confirm the validity of the password change.

The authentication of the user is thus done locally. The secret code is never transmitted to the central terminal over the transmission line. The only transmission of the secret code during the course of the procedure is carried out between the reader of the storage means and the terminal, which limits the risks of interception by a defrauder. The connection to the central system is then made, that is to say, after local verification of the secret code.

Nevertheless, such a procedure requires physical protection of the storage mans (diskette) in order to prevent fraud directly upon the storage means. This implies the utilization of specific materials and technologies, involving relatively high cost.

Description of the invention

The purpose of the invention is to remedy the inconveniences of those procedures described above. For this purpose, it proposes a method for the concealment of a secret code in an authentication device, such as a diskette or a memory card. This procedure permits local verification of the secret code entered by the user, while reducing the risk of attacks by dictionary.

More specifically, the invention concerns a process for the concealment of a secret code in an computer authentication device consisting of the encryption of the secret code by an encryption function in order to form a secret-code image and to store this secret-code image in the authentication device. This procedure is characterized by the fact that it consists, first of all, of the selection of an encryption function which is such that, for each image of the secret code, it will correspond to a plurality of antecedents, all different, of the secret code, but which, once encrypted by the encryption function, will have an image identical to that of the secret code. /4

Advantageously, when the secret code has n characters, the encryptien function will consist of the association of these n characters with an image of the secret code image k having characters, with $k < n$.

According to a preferred execution variant of the invention, the number k of characters of the image of the secret code is equal to $n/2$.

The invention also concerns a method for verification of the secret code of a user desiring to access the central system from a terminal. This user being equipped with an authentication device in which the image of the secret code is concealed by an encryption function, this procedure is characterized by the fact that it comprises a step for local verification of the secret code, entered by the user and encrypted by the encryption function, by comparison with that image of the secret code stored in the authentication device. Then, if that is verified, it comprises a step for verification by the central system.

Brief description of the drawings

- Figure 1 represents, schematically, the distribution of the images of the secret code in memory as well as the possible antecedents of this image;

- Figures 2A, 2B, 3A and 3B show examples of encryption functions applied to a certain number of numeric characters; and /5

- Figure 4 represents the operational procedure for verification of the secret code.

Detailed description of execution variants of the invention

The invention concerns a process for the concealment of a secret code in an authentication device, such as a computer diskette, a memory card or even a pocket calculator.

This process consists of encrypting the secret code, by means of an encryption function g, in order to form an image of the secret code which is then stored in the memory of the authentication device.

The encryption function g is selected in such a way that the image of the secret code will be sufficiently precise for a typing error by the user when entering his secret code to be detected with completely satisfactory probability, even though each image of the secret code will possess numerous antecedents via the encryption function, so that an attack by dictionary will provide numerous false solutions to the local verification function, but not to remote authentication.

In other words, the encryption function g is selected in such a way that the secret code will have a secret-code image which corresponds to a multitude of antecedent codes (referred to merely as "antecedents" in the remainder of the text). These antecedent codes are a sort of false secret codes which, encoded by the encryption function g, all yield the same image of the secret code as the true secret code of the user, but which will be /6 rejected by the authentication procedure.

Thus, a fraudulent user who may happen to be in possession of an authentication device, for example, a diskette, and who would thus have discovered the file of images of secret codes and who, by other means, would also be in possession of the encryption function g, would not be able to determine precisely which is the secret code of the user. In fact, an attack by dictionary would provide him with numerous solutions for the local verification procedure, but a very low chance of finding the true solution, that is to say, the true secret code. Effectively, if the fraudulent user tries one of the antecedent

codes provided by the dictionary attack, it will be verified locally, but will on the other hand be refused by the remote authentication procedure, that is to say, the authentication by the central system.

Represented in Fig. 1, in a highly schematic fashion, is the distribution of the images of secret codes in memory, as well as the distribution of the antecedent codes of these secret-code images.

More precisely, the aggregate of all those codes which could be a secret code chosen by the user are labeled "*E1*" and, with "*E2*", all the images of these secret codes which could be chosen by the user. Group *E1* thus contains all the possible secret codes, including, in particular, a code *x* and a multitude of codes *s1* through *sn*.

If "*g*" is the encryption function selected, then the image of the code *x*, produced by the encryption function *g*, will be the image *X* situated within the group *E2* of images of the possible secret codes. On the other hand, the image of each of the codes *s1* though *sn*, produced by the encryption function *g*, will yield the secret-code image *S* contained in group *E2*.

These are thus all antecedent codes *s1*, *s2*, *s3*,..., *sn* /7 which, encoded by the encryption function *g*, yield an image *S* which also corresponds to the image of the true secret code. It is therefore evident that one of these codes *s1* through *sn* is the true secret code selected by the user. Thus, although all these antecedent codes *s1* through *sn* have an image *S*, one only of these

antecedent codes is the true secret code which will verify the authentication by the central system.

Thus, a fraudulent user in simultaneous possession of both the encryption function *g* and of the image of the secret code *S* will not know which of the antecedent codes *s1* through *sn* to select. Also, if he tries one of the antecedent codes *s1* through *sn* locally, that is to say, at the level of the computer terminal, the verification by the terminal will give him a positive response, that is to say, an authentication process can be implemented. Nevertheless, this authentication procedure will not succeed, and connection to the central system will be refused.

On the other hand, the encryption function is chosen in such a way that it will provide images of secret codes sufficiently precise to permit a typing error on the part of the user to be detected locally, that is to say, without requiring connection to the central system.

According to one execution mode of the invention, the encryption function *g* is a function which associates a secret-code image of reduced size with *n* characters constituting the secret code, that is to say, *k* characters, with $k < n$. For example, for a secret code having *n* characters, the encryption function *g* will associated an image of $k = n/2$ characters. In the preferred execution variant of the invention, the function *g* will assign a secret-code image of four characters (the size being approximately 2^{20} bits) to a secret code of eight /8

characters (which corresponds to a size of approximately 2^{40} bits).

For an encryption function *g* of this type, the user who enters the true secret code with a typing error will have a risk of approximately one million cases (1 in 2^{20}) that his typing error will not be detected during the verification operation. On the other hand, a fraudulent user attempting a dictionary attack will be confronted with approximately one million solutions (2^{20}), among which only one is correct, that is to say, only one will correspond to the true secret code.

It will be evident, of course, that several functions can be utilized to verify those conditions stated above. Even very simple functions can be utilized. For example, if those numbers between 0 and 9 and the letters of the alphabet which represent those values between 10 and 35 are taken into account, it will be possible to select a function *g1* which assigns a value determined between 0 and 35 to each pair of characters (letters or numbers) of the user's secret code, so that the image for a given character of the bigram (that is to say, of the character pair) will be different, when the second character varies. For example, the sum of two characters of the bigram can be selected.

Figure 2A shows, schematically, the treatment carried out by the function *g1* on a secret code containing *n* characters.

Thus seen in Fig. 2A are *n*/2 pairs of characters (*c1*, *c2*), (*c3*, *c4*)... (*c1*, *cn*) and each of the images $Ic_1, \ldots Ic_{n/2}$ of these bigrams. According to the definition of the function *g1*,

described above, each image $Ic_{n/2}$ will correspond to the sum of the characters C_1 and c_n of the corresponding bigram, knowing that, if the sum of the characters yields a value above or equal to 1, the value chosen for $Ic_{n/2}$ will be the value of lowest weight, that is to say, the number of units. /9

Figure 2B shows a numeric example of the encryption produced by means of the function *g1*. Considered in this example is a secret code with eight numeric characters designated *c1*, *c2*,..., *c8*, regrouped into four bigrams whose values are comprised between 0 and 9:

(*c1*, *c2*) = (6, 1)

(*c3*, *c4*) = (5, 7)

(*c5*, *c6*) = (4, 3)

(*c7*, *c8*) = (9, 2)

The function *g1* associates with each bigram the sum of the two characters constituting it. Thus:

Σ (*c1*, *c2*) = 7

Σ (*c3*, *c4*) = 2

Σ (*c5*, *c6*) = 7

Σ (*c7*, *c8*) = 1

It is thus evident from this example that the image of the secret code "61574392" is "7271". Such an image 7271 can have a multitude of antecedents, since each character of the image of this secret code can result from the sum (or of the course the number of units of a number corresponding to the sum) of a multitude of numbers ranging from 0 to 35.

Moreover, it can be seen that, if the user enters the true secret code with a typing error, for example, 7 instead of 6 for the character *c1*, this error will be immediately detected locally, since the sum of 7 and 1 cannot of course yield the /10
number 7 which corresponds to the image *Ic1* of the first pair of characters (*c1*, *c2*).

Presented in Fig. 3A is an example of a different encryption function, the function *g2* which consists of associating the group of eight characters *c1* through *c8*, which comprise the secret code, with four independent linear combinations, modulo 36, of these eight characters, where each linear combination can be different.

For example, the first character *Ic1* of the secret-code image associates the characters *c1*, *c3*, *c4* and *c7* of the secret code; the second character *Ic2* of this image of the secret code associates the characters *c2*, *c5*, *c6* and *c8;* the third character of the image of the secret code *Ic3* associates the characters *c1*, *c2*, *c5* and *c7*, and the fourth character *Ic4* of the image of the secret code associates the characters *c3*, *c4*, *c5* and *c7* of the initial secret code.

The example seen in Fig. 3B is the same as that in Fig. 3A, except that a value has been assigned to each character, which is the same as that given in the example in Fig. 2B. Thus:

c1 = 6

c2 = 1

c3 = 5

c4 = 7

c5 = 4

c6 = 3

c7 = 9

c8 = 2

After encryption, using the function *g2*, of a secret code with eight characters *c1* to *c8*, where *c1*,..., *c8* have the values above, a secret-code image 7007 will be obtained, with *Ic1* = 7, *Ic2* = 0, *Ic3* = 0, *Ic4* = 7.

Thus, the procedure for the concealment of the secret code /11
in the authentication device presents the advantage not only of detecting a possible typing error on the part of the user, when the latter is entering the secret code at the terminal, but above all of preventing an attack by dictionary from a fraudulent user, because the image of the secret code stored on the diskette will have such a large number of possible antecedent codes that a fraudulent user will have very little chance of finding the true secret code.

The procedure described above for the concealment of a secret code on a computer diskette, a memory card or any other authentication device, can be utilized in a process for verification of the secret code entered by a user desiring access to a central system from a terminal connected to a reader capable of reading its authentication device.

For better understanding of the invention, the procedure for verification of the secret code will be described in that case

where the authentication device is a computer diskette.

This verification process consists, after the diskette has been inserted in the diskette reader associated with the terminal, of the entry by the user of his secret code into that terminal from which he wishes to connect to the central system. The terminal then verifies whether the image, produced by the encryption function g, of the secret code s just typed by the user corresponds to the image S stored on the diskette. If that is not the case, the terminal will then refuse any connection to the central system. On the other hand, if it is verified, a step for determination of the unencrypted secret key K is begun, at the end of which the terminal is connected to the central system. This unencrypted secret key K is determined by the password from /12 the inverse f^{-1} of the encryption function f of the key (f being a reversible function), and from the encrypted key stored on the diskette, as explained in patent application FR-A 2,690,257, already cited above.

The authentication procedure which is implemented as soon as the computer terminal is connected to the central system will not be described here, since it is identical to that described in FR-A 2,690,257.

A functional diagram of this procedure for verification of the secret code is shown in Fig. 4.

The computer disk, labeled **10**, is inserted in the computer terminal **14** during a step **e1**. The user, labeled **12**, then enters his secret code (s) in the terminal **14** during step **e2**. A step **e3**

is then carried out, which consists of the encryption, by the function *g*, of the secret code *s* which the user has just entered and then verification of whether the image of the secret code produced by the function *g* indeed corresponds to the secret-code image *s* stored on the diskette **10**. If that is not the case, the verification process is then abandoned (step **e4**), and no verification procedure is executed by the central system. However, if this verification is found to be exact, a step **e4** will be carried out. This step e4 consists of determining the unencrypted secret key *K* and of transmitting it to the central system **16** which will then begin the authentication procedure (step **e5**) by means of an exchange of data with the terminal **14**.

Thus, the procedure for verification of the secret code assures a limitation of the number of connections to the central system, because only those secret codes accepted during the local verification of the secret code become the object of an authentication procedure.

Furthermore, the image of the secret code being stored on /13
the authentication device, and not in a memory accessible to any fraudulent user desiring knowledge of this secret-code image, is first taken up by this authentication device, which contributes to the limitation of frauds.

CLAIMS

1. Process for the concealment of a secret code on a computer authentication device (10), consisting of the encryption of the secret code (*s*) by an encryption function (*g*) in order to form an image of the secret code (*s*) and store this secret-code image on the authentication device, characterized by the fact that it consists, first of all, of the selection of an encryption function (*g*) which is such that, for each stored image of the secret code, it will correspond to a plurality of antecedent codes (*s1*, ..., *sn*), all different, of the secret code, but which, once encrypted by the encryption function (*g*), will have an image (*s*) identical to that of the secret code.

2. Process for the concealment of a secret code according to Claim 1, characterized by the fact that the secret code has *n* characters (*c1*, ..., *cn*), the encryption function (*g*), and that the encryption function (*g*) consists of the association of a secret-image code with *k* characters with these *n* characters (*c1*, ..., *cn*), with $k < n$.

3. Process for the concealment of a secret code according to Claim 2, characterized by the fact that the number *k* of the characters in the image of the secret code is equal to $n/2$.

4. Procedure for the verification of the secret code of a user desiring to access a central system from a terminal, characterized by the fact that, this user (12) being equipped with an authentication device (10) in which the image (*s*) of the secret code is stored by an encryption function (*g*) according to

any of Claims 1 through 3, it comprises a step (e3) for local verification of the secret code, entered by the user and encrypted by the encryption function, by comparison with that image of the secret code stored in the authentication device, and then, if that is verified, a step (e5) for authentication by the central system (16).

FIG. 1

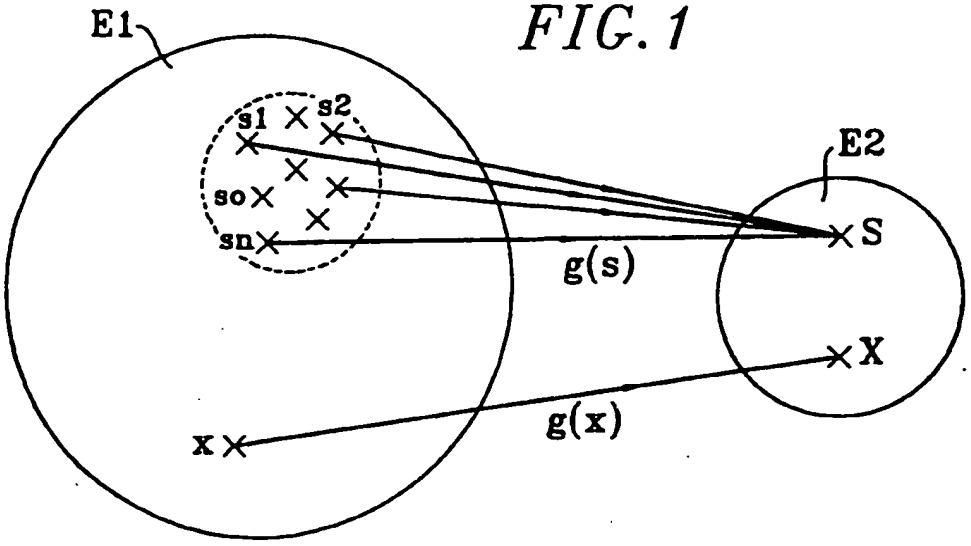
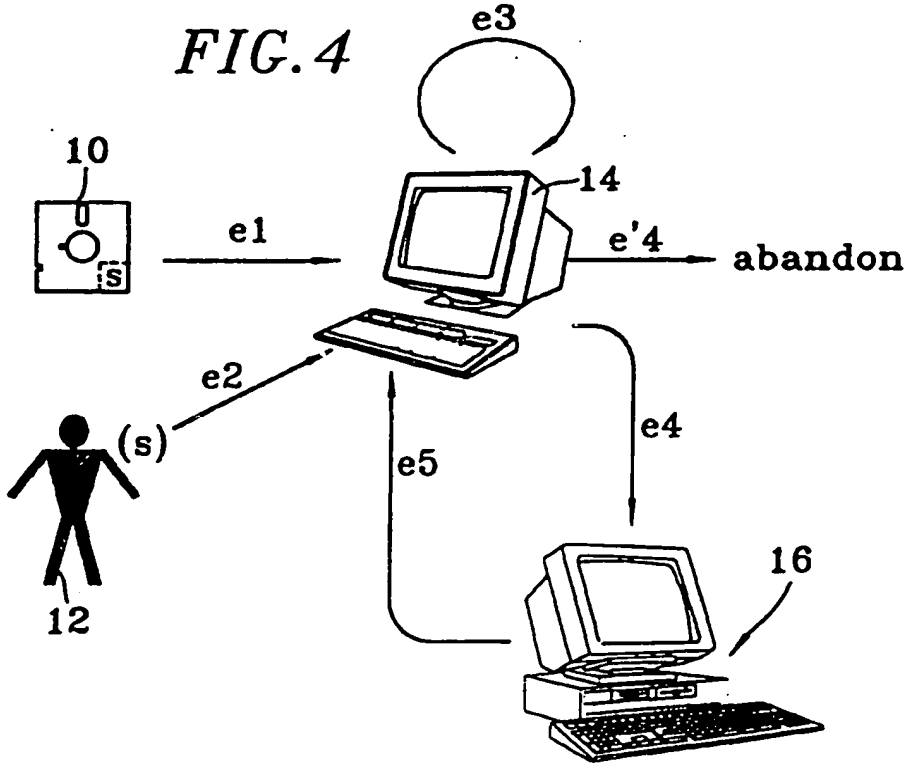


FIG. 4



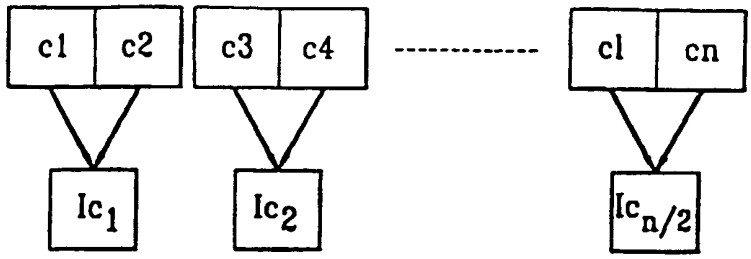


FIG.2A

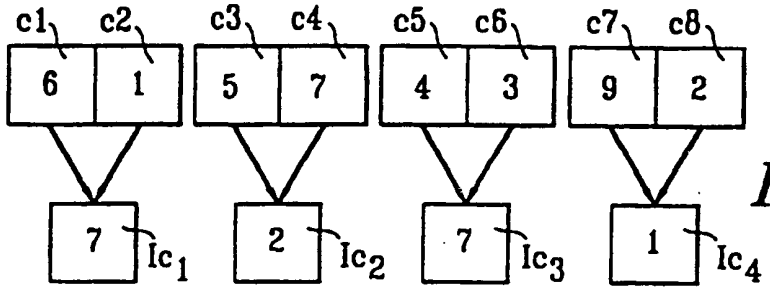


FIG.2B

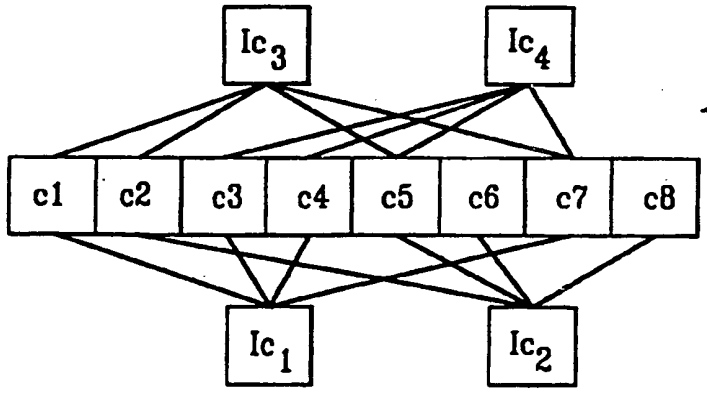


FIG.3A

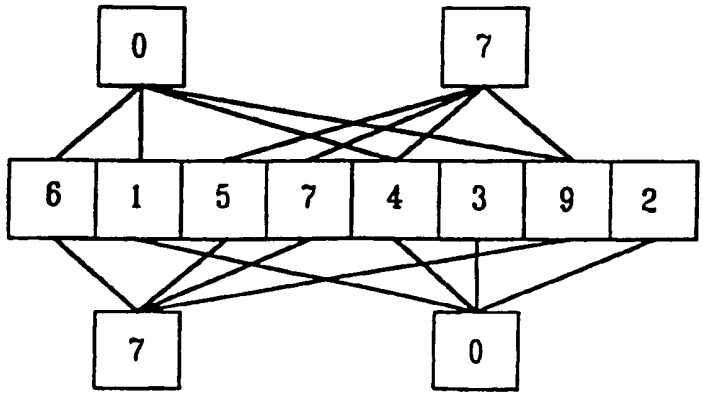


FIG.3B